TABLE OF CONTENTS

C.1 INTRODUCTION

The United States Department of the Treasury, hereafter referred to as “Treasury” or “the Government”, awarded Northrop Grumman, formerly TRW, the Treasury Communications Services (TCS) Contract in 1995. The TCS Contract, which consists of a one-year base plus nine (9) one-year options, expires in September 2005. This solicitation represents the requirements necessary to improve and optimize the network environment currently provided to the Treasury to meet its evolving business needs.

C.1.1 Background

The TCS Contract was designed to provide site-to-site data services for the Treasury by installing multiple high-speed networks to support applications that include upgraded e-mail, electronic commerce, security services, and videoconferencing. The requirements of the contract were later modified to include outsourced services from commercial carriers in place of installation of a private backbone network. Currently, Northrop Grumman is responsible, through the TCS Contract, for the oversight and management of multiple data communications carriers for service delivery, trouble resolution, and billing functionality.

The TCS Contract is a department resource that will provide data communications products along with a centralized network and management system. TCS is the largest private, secured civilian government network in the United States. There are currently over 1000 locations connected to TCS, supported by over 4200 circuits. The majority of the sites are in the continental U.S.; however, coverage also extends to other global locations including sites in Guam, Europe, Bermuda, and the Bahamas. Exhibit 1 below represents the current footprint of the TCS Network. Reference Section J, Attachment J-2 of this solicitation for a complete listing of the TCS sites as of February 2004.

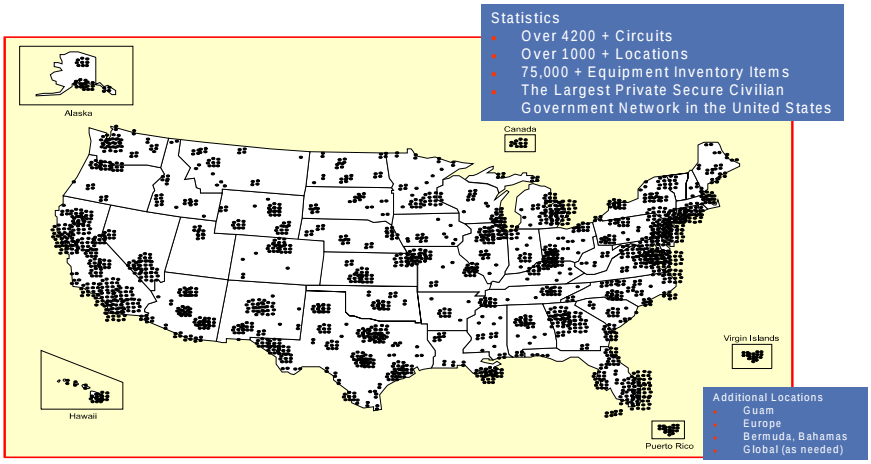


Exhibit 1: Department of the Treasury’s TCS Network

The Treasury is seeking replacement and/or enhancement of services now provided through the TCS Contract. The contract awarded from this solicitation will replace TCS and has been assigned a new name, Treasury Communications Enterprise (TCE). The new TCE Contract shall replace the existing TCS Contract as an improved, cost effective, and technically responsive contract. TCE shall replace TCS prior to its expiration on September 27, 2005.

Treasury currently has multiple Bureaus with independent telecommunications networks, all of which are connected through a distributed hub-and-spoke architecture. A nationwide network connects multiple Government Bureau nodes through high-speed connections. In turn, the Bureau nodes connect to various Bureau offices. See Section J, Attachment J-3 for network architecture.

C.1.2 Strategic Direction

The TCE operational capability should be a framework for developing a Treasury-wide Secure Enterprise Network for enabling the convergence of data, voice and video technologies into a single network infrastructure that supports the efficient operation of applications and services across the entire Treasury operating environment. This converged communications transport framework will allow the Treasury and its Bureaus to build secure, robust, eGov-enabled business solutions. The desired operating capabilities for the Treasury-wide secure enterprise network are as follows:

a) Allow for the operation of data, video, voice and other multimedia services across a single, common enterprise network infrastructure that supports both real-time [Voice over Internet Protocol (VoIP), video conferencing, etc.] and non-real-time applications

b) Employ the latest network perimeter detection appliances and network access protection devices that will secure Treasury information and data from unauthorized access and intrusion both externally and internally

c) Accommodate the deployment and integration of e-Government and Treasury-wide enterprise applications across the entire Department operating environment through standardization on Internet Protocol (IP)-based services while allowing for the operation of legacy environments, such as Systems Network Architecture (SNA), until the various business application modernization programs within the Treasury and its Bureaus have been completed

d) Maximize the crisis and business operation of the Treasury and its Bureaus in times of disaster and national crises regardless of damage to the public switched telephone and telecommunications carriers' connection-oriented networks

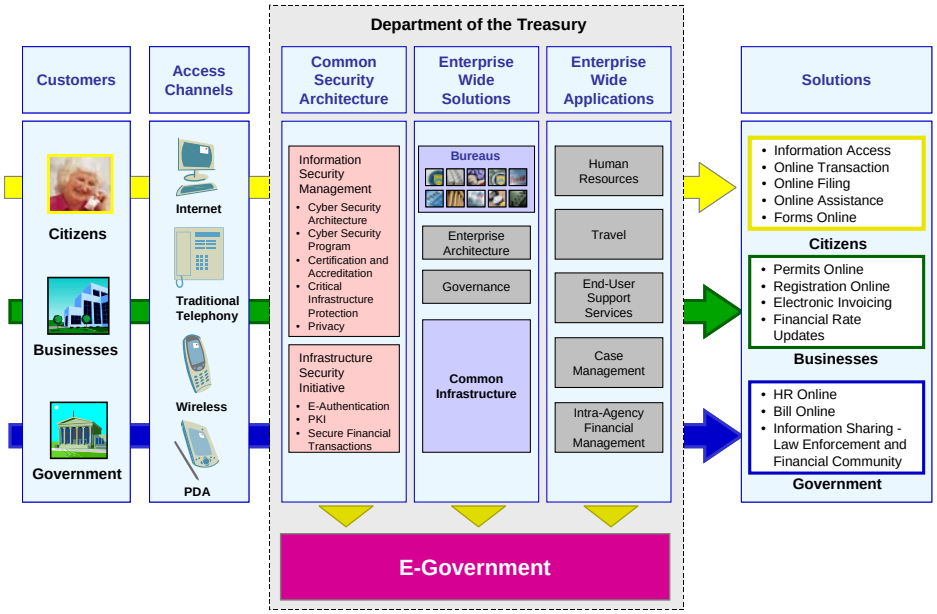
e) Reduce telecommunication infrastructures total cost of ownership through the deployment of a single enterprise network infrastructure and standardization on the internationally sanctioned Internet Protocol (IP) standards

f) Support secure enterprise mobility via telecommuting and teleworking by providing secure, certificate-based remote access

C.1.3 TCE Goals and Objectives

The objective of the TCE Contract is to employ a next-generation enterprise network that enhances performance of common enterprise wide application services across the entire Treasury operating environment. This may entail the enhancement, replacement, or consolidation of the existing network infrastructure and its associated service support assets and facilities. Furthermore, the TCE Contract is expected to provide enterprise-wide managed services across the Treasury operating environment. This contract includes a provision for taking advantage of new emerging technology in enabling new business requirements and needs.

Exhibit 2: Program Vision



In addition, the TCE Contract shall support future Government information technology (IT) requirements by employing converged technologies, such as VoIP, unified messaging, and IP-based desktop video/audio conferencing and electronic collaboration. Accordingly, TCE goals and objectives include the following:

1. Allow for on demand growth for all enterprise telecommunication services across the entire Treasury operating environment in an cost effective and operational efficient manor

2. Enable secure remote access to Treasury data from Continental U.S. (CONUS) and Outside CONUS (OCONUS) locations

3. Employ performance based managed services for highly reliable and secure telecommunication and provisioning services that meet or exceed customer expectations and performance metrics as identified in Section F of this SOW

4. Provide an effective, efficient, and interactive management information system that provides comprehensive, accurate, and timely information on telecommunications services provisioning, program status, performance, and billing

5. Ensure that the enterprise-wide telecommunications services support Treasury's compliance with e-Government initiatives and Government standards and policy requirements outlined in Clinger-Cohen Act, Treasury enterprise architecture, and federal security policies

6. Insure the transition to the next-generation telecommunications infrastructure is seamless and transparent to user without disruption of existing services

7. Effectively utilize subcontract and teaming arrangements, including use of small disadvantaged, woman-owned, veteran-owned, HUBzone and service-disabled veteran businesses

C.1.4 High-Level TCE Vision

The Treasury's Chief Information Officer (CIO), in conjunction with Bureau CIOs, developed a high-level vision for TCE. That vision calls for a single, seamless, department-wide WAN, to be serviced under one contract. In this manner, TCE will allow the Government to offer scaleable, world-class, customer-focused services in support of mission-critical and other daily Government activities. The Government envisions that a centralized network, with established and consistent standards and interfaces, will reduce the management burden of the network and will allow for greater interoperability through a consolidation of vendors and vendor products. Ultimately this managed service approach should prove a less-expensive alternative to the current set-up and enable Government staff to better focus on its core mission.

This vision comprises three essential elements: technology, support, and management. These elements are specified to ensure multiple objectives are met. The technology and services offered must be in line with the future needs and requirements of the Government and the TCE customer. The TCE program will facilitate growth and expansion, while allowing for maximum flexibility within the program. User satisfaction will be enhanced, while mission critical and daily activities are supported through predefined service levels.

The first element, technology, shall meet current service needs and support the eventual convergence of Treasury's data, voice, and video networks. Technology should provide for secure and resilient services that support established disaster recovery plans. The second element, support, shall target customer-centric activities such as ordering, billing, and trouble management, all within a managed services environment. In general, all support services should be designed to simplify the customer's interactions and create an easy to use program. The third element, management, shall facilitate consolidation of oversight processes and procedures and, more importantly, set the groundwork for the TCE business model.

The TCE business model is based on a managed services concept where a single utility for voice, data, video, and wireless services is provided in a fee-for-services environment. Within the TCE business model, services will be provided based on a combination of site type, required availability, and class of service (CoS). In addition, this business model includes incentive-based service delivery, an objective that is gaining more prominence as the Federal Government gradually adopts performance based contracting methodologies. Per this objective, incentives are used to create motivation for providing improved services. These incentives ultimately create increased customer satisfaction, a critical aspect of the TCE vision.

C.1.4.1 TCE Features, Future Services, and Benefits

The Treasury-wide Secure Enterprise Network infrastructure is the framework that will support Treasury enterprise and Bureau specific IP-based applications. Examples of future service offerings that will rely on the TCE network may include, at a minimum, the following:

Features	Application/Service	Benefit
• Virtual Private Networks • IP Service Center • Metadata Directory • IP Based Transport • Advanced Security Appliances • IP QoS • IP Multicast • Common Enterprise Secure Public Internet Gateways • Legacy network protocol support • IP/MPLS enabled Network • IPv6 • Packet-switched connectionless architecture • Centralized, Virtual Enterprise Network Management	• IP Telephony (VoIP) • IP Video Conferencing • IP-based TV Service	• Content Networking • Enterprise Mobility • Workforce Optimization • e-Learning • Customer Care • e-Commerce • Enable Web Portal Technology • Enable Active Directory and Single Sign-on • Telecommuting • Remote Access • PKI Enabled • High Availability Network (SONETx, Wavelength Service, etc.)

This network infrastructure should provide the following benefits based on deployment of this cohesive infrastructure framework:

a) Robust service availability – increased uptime due to robustness of a high speed, robust, packet-switched network

b) Rapid deployment and mobility – operating on standards-based protocols and deploying consistent IT media services across the Treasury enterprise will allow for universal rapid deployment of applications in support of Government business operations

c) Maximum operating flexibility – operating across standards-based IP networks allows for easy transition to changing business requirements and emerging technology

d) Seamless interoperability – employment of standards-based network infrastructure allows for seamless operations and easier integration of applications across the network infrastructure landscape

e) Operational simplification – allows for streamlining network operations and management through remote systems monitoring and restoral management; building and campus customer premise equipment will be operated unattended and restored through remote access by expert technicians distributed throughout the telecommunications infrastructure support center system

f) Reduced infrastructure and services cost – convergence of voice, data, and video will result in the consolidation of infrastructure and collapsing organizational management structures into a single service management entity

C.1.5 Treasury Mission

The Treasury is the financial manager for the U.S. Government and a world leader in formulating and shaping economic policies and financial practices. The essential mission and functions of the Treasury are summarized as follows:

a) Promote prosperous U.S. and world economy
b) Promote a stable U.S. and world economy
c) Effectively manage the U.S. Government's finances
d) Maintain, manage, and preserve the economic and financial management institutions of the United States, including all monetary, credit, and financial systems
e) Serve as a principal economic advisor to the President
f) Perform international economic and monetary control as it pertains to the well-being of the Nation
g) Manufacture currency, coins, and stamps
h) Establish, monitor, and track methods of currency exchange and financial transactions

C.1.6 Treasury Strategic Direction

The Treasury, as the financial manager for the U.S. Government and a world leader in formulating and shaping economic policies and financial practices, has five (5) strategic goals. Each strategic goal has supporting strategic objectives. The goals and objectives describe how Treasury will manage and influence the U.S. and international economic and financial systems so that they operate at their full potential, maintain stable foundations for growth, and preserve the integrity of their systems and operations.

a) Promote Prosperous U.S. and World Economies: ensure that the United States and World economies perform at full economic potential

b) Promote Stable U.S. and World Economies: create conditions which allow the American people to feel economically secure to live as they desire, and are protected from financial frauds and other crimes

c) Preserve the Integrity of Financial Systems: ensure that the U.S. financial systems will continue to operate without disruption; keep the systems free and open to legitimate users, while excluding those who wish to use the system for illegal purposes; and ensure that the U.S. financial systems and access to U.S. goods and services are closed to individuals, groups, and nations that threaten the nations vital interests

d) Manage the U.S. Government's Finances Effectively: manage the Nation's finances by collecting money due the United States, making its payments, managing its borrowing, performing central accounting functions, and producing coins and currency to meet demand; serve as the primary federal tax collecting agent and collector of revenue on regulated commodities

e) Corporate Guidance: provide guidance for the internal operation of the Department of the Treasury and strategic direction for achieving the President's Management Agenda

C.1.7 Treasury Organization

The Department of the Treasury is organized into two major components, the Departmental Offices (DO) and mission Bureaus, including associated nation-wide field offices. The DOs are primarily responsible for policy formulation, while the Bureaus are primarily operating organizations that execute many of the Treasury's goals. The majority of Treasury's workforce and resources are focused in its operating Bureaus.

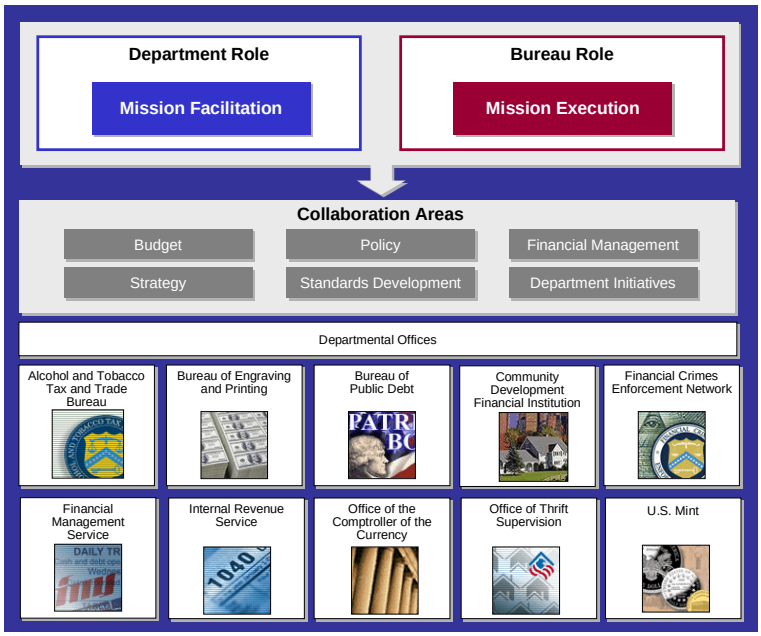


Exhibit 3: Treasury Organization

C.1.7.1 Departmental Offices

DO is composed of divisions, as described below, headed by Assistant Secretaries, some of whom report to Under Secretaries, with primary responsibility for policy formulation and overall management of the Treasury.

a) Domestic Finance develops policies and economic guidance, which help create the conditions for domestic prosperity through advice and assistance in domestic finance, banking, financial institutions, federal debt finance, financial regulation, and capital markets.

b) The Office of Economic Policy is responsible for analyzing and reporting on current and prospective economic developments in the U.S. and world economies and assisting in

the determination of appropriate economic policies, which strongly influence conditions for prosperity abroad.

c) The Executive Office of Terrorist Financing and Financial Crime develops and implements U.S. strategies to combat terrorist financing domestically and internationally; develops and implements the National Money Laundering Strategy as well as other policies and programs to fight financial crimes; administers the Treasury Forfeiture Fund through the Executive Office for Asset Forfeiture; implements strategies to administer and enforce economic and trade sanctions based on U.S. foreign policy and national security goals through the Office of Foreign Assets Control, which enforces economic and trade sanctions based on U.S. foreign policy and national security goals, as well as implements sanctions against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction

d) The Office of International Affairs advises and assists in the formulation and execution of U.S. international economic and financial policy, including the development of policies for international financial, economic, monetary, trade, investment, bilateral aid, environment, debt, development, and energy programs; develops policy for the U.S. participation in international financial institutions

e) Tax Policy develops and implements tax policies and programs; reviews regulations and rulings to administer the Internal Revenue Code; negotiates tax treaties; and provides economic and legal policy analysis for domestic and international tax policy decisions; provides estimates for the President's budget, fiscal policy decisions, and cash management decisions

Internally, DO is responsible for overall management of the Department. Offices responsible for the internal management and controls include General Counsel, the Assistant Secretary for Management and Chief Financial Officer, Public Affairs, and the Treasurer of the United States. Also, inspector general functions provide independent audits, investigations, and oversight to the Treasury and its programs.

C.1.7.2 Treasury Bureaus

There are ten (10) Treasury Bureaus, as described below, with specific missions and goals that have been developed to carry out the overall missions of the Treasury.

a) The Alcohol and Tobacco Tax and Trade Bureau (TTB) administers and enforces laws on the production, use, and distribution of alcohol and tobacco products, and also collects excise taxes for firearms and ammunition.

b) The Bureau of Engraving and Printing (BEP) designs and manufactures U.S. currency, many stamps, securities, and other official certificates and awards.

c) The Bureau of the Public Debt (BPD) borrows the money needed to operate the Federal Government and accounts for the Public Debt, which it administers by issuing and servicing U.S. Treasury marketable, savings, and special purpose securities.

d) The Community Development Financial Institutions (CDFI) Fund expands the capacity of financial institutions to provide credit, capital, and financial services to underserved populations and communities in the United States (CDFI is not a Bureau but has special program emphasis).

e) The Financial Crimes Enforcement Network (FinCEN) collects, analyzes, and shares information needed to combat the financial aspects of criminal activity worldwide.

f) The Financial Management Service (FMS) provides central payment services to federal program agencies, operates the Federal Government's collections and deposit systems, provides government-wide accounting and reporting services, and manages the collection of delinquent debt.

g) The Internal Revenue Service (IRS) is the largest of Treasury's Bureaus and determines, assesses, and collects internal revenue in the United States.

h) The U.S. Mint designs and manufactures domestic coins as well as commemorative medals and other numismatic items, as well as distributes U.S. coins to the Federal Reserve Banks and maintains physical custody and protection of silver and gold assets.

i) The Office of the Comptroller of the Currency (OCC) charters, regulates, and supervises national banks to ensure a safe, sound, and competitive banking system that supports the citizens, communities, and economy of the United States.

j) The Office of Thrift Supervision (OTS) charters, examines, and regulates federal thrifts to maintain their safety and soundness, and regulates state-chartered savings associations belonging to the Savings Association Insurance Fund and savings association affiliates and holding companies.

C.1.8 Description of Current Environment

The current TCS network, as depicted in Exhibit 4 below, is an aggregation of Bureau networks and sub-networks partitioned off of a Treasury backbone network employing an array of multiple star and tiered topologies for connecting Treasury operating sites and field offices with Bureau management structures and the Department of Treasury Headquarters. The current environment also employs more than 215 different customized system interfaces and customer premise equipment (CPE) sets with no consistency in standardization. The managed service approach outlined in this SOW should provide a less-expensive alternative to the current set-up of a "network of networks and sub- networks" with an array of customized system interfaces while allowing Treasury and its Bureau staffs to better focus resources on their core mission and services to the public. Furthermore, the future service should optimize the operation and performance of the enterprise-wide applications services across the entire Treasury operating environment.

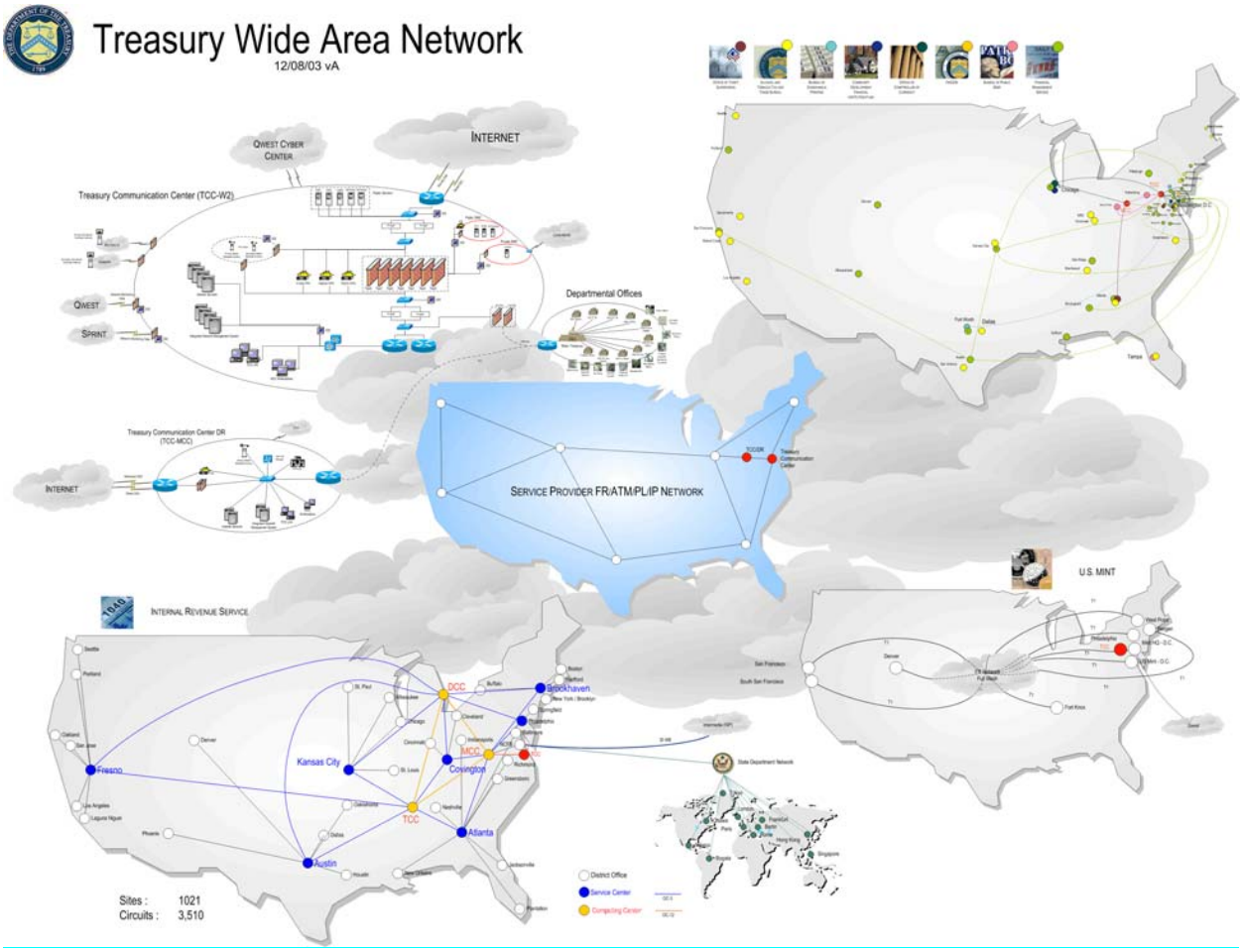


Exhibit 4: Logical Representation of Treasury's Current Network

C.1.8.1 Current Infrastructure Assets

The current TCS network infrastructure assets are owned by the Government, and have been purchased under multiple contracts and with varying terms and conditions. The Contractor shall accept title of all TCS network assets (switches, routers, and similar network equipment). The Contractor may make use of any equipment it deems useful in providing network connectivity and managed services, and will be responsible for disposing of any unused equipment. A list of TCS equipment is supplied in Section J, Attachment J-4. See H.17 *Exchange/Sale*.

C.2 SCOPE

The managed, enterprise-wide IT services to be offered though the TCE contract shall be made available to all of the Treasury, including departmental offices, Bureaus, regional agencies, and field offices (hereafter referred to as "Bureau"). TCE shall support each Bureau located in the United States or in any of its territories that is currently supported by TCS, regardless of its size or geographic location. Bureaus that TCS does not currently support may opt to use this contract in the future.

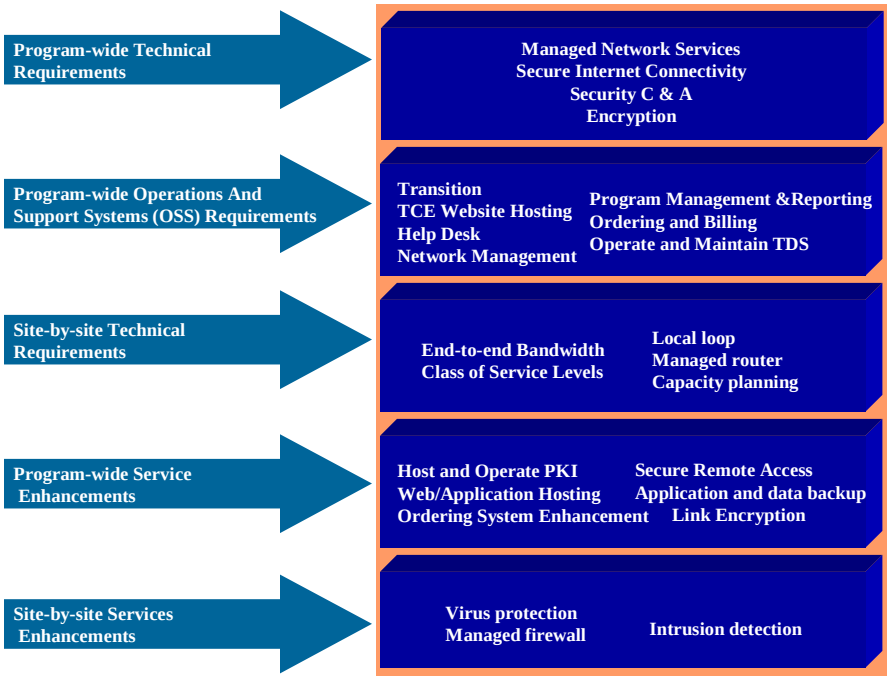
The scope of work under TCE shall include the planning, design, transition, implementation, operation, maintenance, and management of the TCE WAN. All equipment required to provide TCE services will be owned, managed, monitored and maintained by the service provider to meet the service levels specified in Section F. The Contractor will provide all facilities necessary to provide TCE services, including a secure operations center. The Contractor will be responsible for providing multiple contract deliverables that are defined in the following paragraphs of this SOW. For a list of deliverables, see Section C.6. All services shall be provided in accordance with the service levels specified in Section F, *Deliveries and Performance*.

Additionally, the scope of the contract shall include new requirements that may develop as a result of technology advancements and changing business needs. The TCE Contract shall support the Government's future requirements for deploying converged technologies such as VoIP, unified messaging, and IP-based desktop video/audio conferencing and electronic collaboration. Additionally, some current Treasury IT projects such as DTS2/DTS3, VMS, etc., might be migrated into the TCE Contract in the future.

TCE shall provide core and optional services under five distinct categories:

1. Program-wide technical services
2. Program-wide Operations & System Support (OSS) services
3. Site-by-site technical services
4. Program-wide enhanced services
5. Site-by-site enhanced services

Figure C-1: TCE Core and Enhanced Services



In addition to the services mentioned in Figure C-1, the scope of TCE shall include other program and contract management services outlined further in this document.

C.3 CORE REQUIREMENTS

C.3.1 Core Program-Wide Technical Requirements

C.3.1.1 Provide Managed Network Services Program-Wide

TCE shall provide fully managed end-to-end (demarc-to-demarc) WAN services between and among various Treasury, Government, and commercial locations in the United States, the U.S. Territories, and internationally. Figure C-2 below depicts the demarcation point for any typical TCE site. Section J, Attachment J-2 provides a list of all TCE Treasury and Bureau sites requiring telecommunications services that are specifically known at the time of this document. The list includes Government sites in Alaska and Hawaii and in overseas U.S. Territories in Puerto Rico, Guam, the Virgin Islands, Bermuda, and the Bahamas, as well as selected sites in Canada. In addition, the Government may request the addition of new sites as needs dictate.

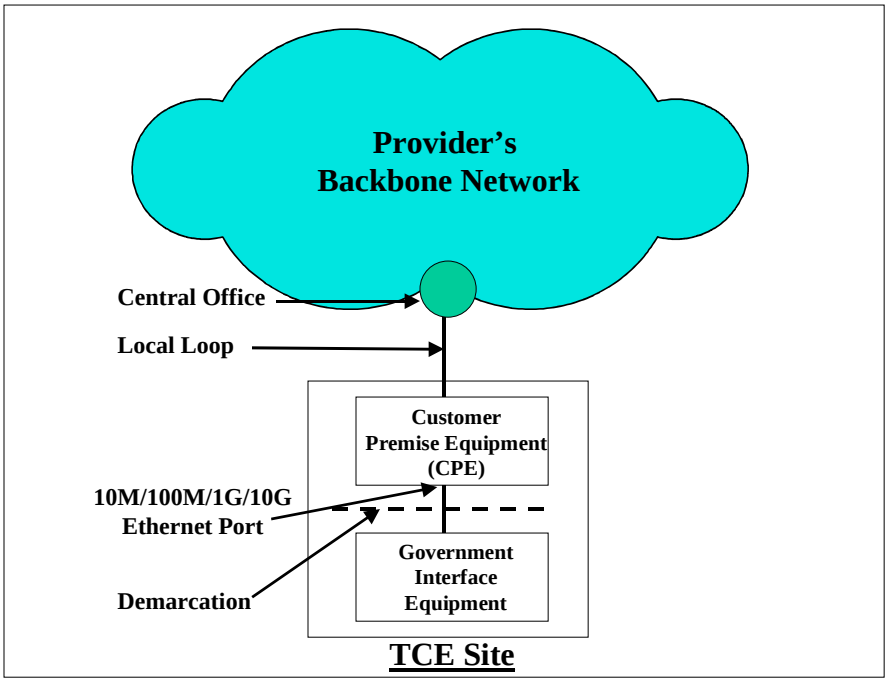


Figure C-2: Demarcation Point

The Contractor shall provide transport connectivity to all TCE sites in order to achieve seamless communications among the sites and with the Internet. The transport components shall typically include the facilities, hardware, and software necessary to provide connectivity and

operability to all Government sites connected to the TCE WAN, and to provide any of the services described herein.

The services shall typically include bandwidth management, traffic analysis, network monitoring, ensuring network availability, ensuring security, access control, web-based ordering and billing, management reporting, and other services as described in this document. The Contractor shall maintain the infrastructure necessary to provide these services at their cost, and shall include all charges to the Government for the managed services in the Contract Line Items in Section B. FigureC-3 depicts a sample Contract Line Item Number (CLIN) structure, which illustrates the various managed services components that shall be included in the CLINs.

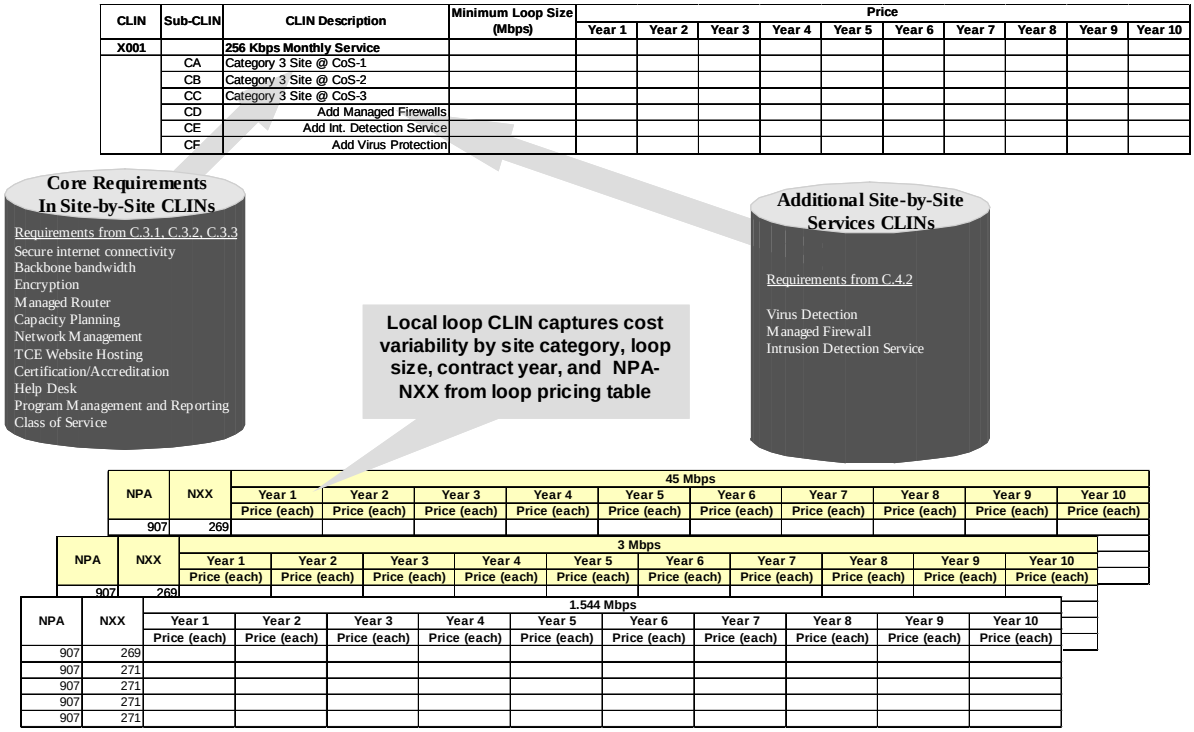


Figure C-3: Sample CLIN Structure

The Contractor shall use TCS and non-TCS baseline IP-based network services data to design the TCE architecture. Appropriate TCS and non-TCS IP-based network services data will be available to the Offerors for reference via a secure Government as identified in Section L.6, *Solicitation Copies and Disclosures*. Additional information for successfully accomplishing the transition from TCS to TCE will be made available to the Contractor during the post-award period.

Additionally, TCE is a performance-based contract. The performance measures, their definitions, and the Service Level Agreements (SLAs) are provided in Section F. The

Contractor shall agree to provide managed network and security services to TCE in accordance with SLAs defined in Section F.

C.3.1.1.1 Provide Sufficient Capacity to Support Use of Treasury-wide Applications

The Government wishes to ensure that the TCE WAN supports the efficient use of Treasury's department-wide applications. The Contractor shall provide WAN connectivity to data centers, computing centers, and similar locations at sufficient capacities to support use of applications hosted at these sites and shall ensure a minimum of 99.99% availability. These sites are listed in Section J, Attachment B-2 as site category 1 locations. The Contractor shall provide WAN connectivity to all other sites at sufficient capacities to support the data connectivity needs of those sites. The Contractor shall provide connectivity such that it supports all IP-based applications on the Contractor's core backbone network and SNA traffic on point-to-point private links with link encryption. Details on the current level of services used per site will be available to the Contractor for reference via a secure Government website, as identified in Section L.6, *Solicitation Copies and Disclosures*.

C.3.1.1.2 Provide TCE Secure Network Operations and Management Services

The Contractor shall provide secure network operations and management services to the Government. The Contractor shall ensure that all Government equipment and traffic shall be either physically or logically separated from Contractor's other non-TCE equipment and customer traffic. Additionally, TCE equipment and data should not be accessible or viewable by any unauthorized non-TCE personnel at the Contractor's Network Operations Center (NOC). See also C.3.2.6, *Provide Help Desk Support*.

C.3.1.2 Ensure High-Level of Security

The Contractor shall meet all Federal Government and Treasury security requirements and standards for network, communications, and system protection for all TCE services provided to the Government. The Contractor shall ensure the confidentiality and integrity of Government user profiles and data transiting the TCE WAN. Additionally, the Contractor shall implement all Government Information Assurance mandates as specified in those documents identified in Section C.3.1.2.1.

C.3.1.2.1 Comply with Policies and Procedures

The Contractor shall comply with Government-wide and Bureau-specific security policies, including but not limited to the following:

1) TDP 71-10 and IRS IRM 25.10 relating to personnel security and remote access,
2) TDP 85-01 and IRS IRM 1.16 relating to physical security,
3) Presidential Decision Directive 63 (PDD-63), Executive Order 13231 (EO 13231), and Federal Preparedness Circular 65 (FPC-65), relating to critical infrastructure protection (CIP),
4) The Privacy Act,
5) The Office of Management and Budget [e.g., OMB Circular A-130, Appendix III; OMB guidance for compliance with the Federal Information Security Management Act (FISMA) of 2002],

6) The Government Accounting Office (e.g., *Federal Information System Control Audit Manual (FISCAM)*, GAO/AIMD-12.19.6),
7) The National Institute of Standards and Technology (NIST) Special Publications, in particular the 800 series, and Federal Information Processing Standards (FIPS), and Cryptographic standards),
8) USC 44, Chapter 35, The Federal Information Security Management Act (FISMA) of 2002.

Additionally, the Contractor shall comply with all new versions, amendments, and modifications made to the above-mentioned documents/standards, if and when they become applicable in the future.

Note: Web links are provided in Section J, Attachment J-10 where vendors can access these documents.

C.3.1.2.2 Pass Network Certification and Accreditation (C&A)

The Contractor shall contract with an independent firm to obtain certification and accreditation (C&A) of TCE systems at each site within the FISMA-mandated three-year cycle of C&A activities. The Contractor shall provide evidence of security compliance via site documentation from the third party vendor that is responsible for C&A of TCE systems and the network. The Government reserves the right to approve the independent Contractor following contract award. Additionally, irrespective of the C&A performed by the independent contractor the Government retains the right to perform an independent inspection of the system using Government employees or an independently retained firm.

The Contractor shall provide C&A documentation as defined within the NIST SP 800 series guidance to the Government ten (10) working days in advance of the C&A due date, not including between December 1 and January 5 each year (unless specifically requested during that time by the Government) for review. The Government will provide written acceptance, comments, and/or change requests, if any, within fifteen (15) working days from receipt by the Government.

The Contractor shall provide documentation on how its proposed solution is protected against active and passive network intrusion or compromise attempts.

After transitioning to the TCE network, the Contractor shall deliver to the Government a written evaluation of any proposed logical or physical system modifications (or interconnections) that could affect the security posture of TCE. The Contractor shall not implement such changes without prior Government approval. System modifications deemed by the Government to be significant will require updates to any relevant security documentation and potential re-accreditation by the Government consistent with federal law, FISMA and OMB guidelines such as A-130.

C.3.1.2.3 Conduct Security Tests and Evaluations

The Contractor shall develop and execute the Security Test and Evaluation (ST&E) Plan and associated procedures included as part of the C&A documentation, as described in paragraph C.3.1.2.2 and specified by NIST 800. The ST&E Plan shall be provided to the Government

within 60 days of notice to proceed for the Government's approval and shall be executed within a year from the date of approval. The Contractor shall ensure that C&A and ST&E for TCE has been successfully conducted prior to transition of any site to TCE and has been appropriately updated once the sites have been cutover from TCS to TCE.

The Contractor shall provide the technical analysis of the raw data results from the execution of the ST&E Plan and procedures. The Contractor shall write the test report, document the results, and provide any technical narrative that may be required in support of any C&A activity. The Contractor shall support site security assessment visits and operational testing as required by the Government. The Contractor shall document security related findings and recommendations from the ST&E Plan in the ST&E Results document, and update the Plan of Action and Milestones as required.

C.3.1.2.4 Ensure Continuity of Operations & Disaster Recovery

The Contractor shall develop and submit to the Government for approval the TCE Disaster Recovery (DR) and Continuity of Operations (COOP) Plans within 60 days of notice to proceed. The approved TCE DR and COOP Plans will be implemented within six (6) months of their approval. The Contractor shall update the plans as necessary or at least on a semi-annual basis to ensure that they reflect any changes made to the C&A or ST&E documentations. The plans shall be based upon the data contained in the C&A security documentation, as described in paragraph C.3.1.2.2.

The TCE DR Plan (TCE-wide and Bureau-specific) shall address disaster recovery at both TCE-wide and Bureau-specific levels. The TCE DR Plan, at a minimum, shall describe in detail the method by which service will be restored or maintained under a number of emergency situations. The plan shall document recovery procedures in the event of catastrophic loss of single and/or multiple transmission facilities and/or related equipment required to deliver managed services. The plan shall specify emergency maintenance actions with stated response intervals. The plan shall identify key infrastructure sites and corresponding minimum bandwidth requirements, as well as procedural mechanisms for activating the plan. The DR Plan shall also address training for TCE and Contractor staff and Government personnel, at a minimum covering those persons and functions identified in the Government DR Plan.

The Contractor shall plan and conduct regular DR exercises in conjunction with Government testing of their enterprise disaster recovery plans, in order to validate the feasibility and efficacy of the DR Plan (TCE-wide and Bureau-specific). The Contractor shall provide test data and documentation for independent validation and verification of all DR tests.

The COOP Plan shall contain the Contractor's business functions determined as essential for executing TCE's core mission and the means (process, procedures, and resources) by which those functions shall be sustained (either in place or in a recovery site) throughout emergencies of various severity. The COOP Plan shall also identify personnel necessary to ensure those processes.

C.3.1.2.5 Screen Personnel

The Contractor shall provide personnel security in accordance with TDP 71-10 Chapter II Section 4 (Treasury Communications System Contractor Employee Personnel Security and Investigations Policy). Contractor personnel administering or maintaining the system will be

required to meet the level of trust for communication on the network. At a minimum, Contractor personnel will be required to complete an SF-85P Public Trust Questionnaire.

At the Government's request, the Contractor shall provide appropriate personnel that are able to pass minimum or full background investigation for access to Government facilities, at no additional cost. The Contractor shall ensure that any personnel working on TCE development, implementation and maintenance shall have unescorted access to Contractor operated TCE facilities and must be a United States citizen.

The Contractor shall provide security awareness information and training on a yearly basis to all Contractor staff working on the TCE program.

C.3.1.2.6 Authenticate Traffic and Control Access

The Contractor shall provide a centrally managed method for all authorized Government and assigned Contractor personnel to access the TCE network. This method shall enforce proper authentication and non-repudiation, based on explicitly assigned user and groups rights. The access solution shall be compatible with the existing Government and Bureau systems and environments.

C.3.1.3 Provide Secure Internet Access Services

The Contractor shall provide secure Internet access to all TCE sites in accordance with Government's secure Internet access and network perimeter security policies. The Contractor shall provide multiple Internet access points to ensure that the system is robust and highly available.

The Contractor shall ensure that only the public IP addresses for public Government web servers located within the demilitarized zone, or DMZ, are available via the primary Domain Name System (DNS) server. All other Government servers, internal web sites (intranet), and client workstation IP addresses will be protected by network address translation (NAT) or port address translation (PAT) at the DMZ innermost boundary when making inbound or outbound Internet connections.

C.3.1.3.1 Perimeter Firewall Protection For Internet Traffic

The Contractor shall provide firewall services to ensure the integrity of the TCE services and network. The Contractor shall ensure that all Government public servers are operated within a DMZ.

The Contractor shall ensure that a NAT scheme will be applied at the firewall, which provides the innermost boundary for all down stream non-public Web servers and client workstations.

The Contractor shall ensure that the default setting for all firewall ports with inbound or outbound access to the Internet is "deny" or its functional equivalent.

The Contractor shall ensure that only authenticated inbound traffic on explicitly approved ports will be allowed to establish connections to Government workstations and servers.

The Contractor shall monitor all inbound and outbound connections and traffic at the firewall boundaries and shall generate audit logs, which shall capture at a minimum source and destination IP address, date and time, and other relevant system information. These audit logs shall be available for Government review for a period of five (5) years. The Contractor shall provide all audit logs to the Government upon Contract completion.

The Contractor shall provide firewall solutions that provide, stateful inspection and application of proxy-based services. Other firewall inspection methods may also be used to ensure network integrity.

The Contractor shall ensure that the firewalls have the capability to filter based on all of the following:

a) Transmission Control Protocol
b) User Datagram Protocol
c) IP addresses
d) Incoming network interfaces

The Contractor shall ensure that the firewall shall block all inbound traffic unless that traffic is explicitly permitted.

The Contractor shall ensure that the firewall solution shall support a centralized policy management solution.

The Contractor shall filter inbound traffic to the TCE Network to reject the following:

a) Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself
b) Inbound traffic with a source address indicating that the packet originated on a network behind the firewall
c) Inbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks
d) Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic
e) Inbound traffic containing IP source routing information
f) Inbound or outbound network traffic containing a source or destination address of the local host
g) Inbound network traffic containing a source address of 0.0.0.0 or outbound containing a destination address of 0.0.0.0
h) Inbound or outbound traffic containing directed broadcast addresses

The Contractor shall ensure that the firewall shall support centralized user authentication and centralized security event logging.

C.3.1.3.2 Intrusion Detection Services

The Contractor shall monitor the TCE network infrastructure using intrusion detection system (IDS) technologies which provide for the detection of signature, anomaly behavior events or use any other federally approved detection method to provide coverage from the TCE network

perimeter up to and including all critical network nodes. Additionally, the Contractor shall provide an IDS data feed to the Government Security Operations Center or SOC.

C.3.1.3.3 Provide Virus Protection

The Contractor shall provide virus protection for all inbound traffic from the Internet. All inbound traffic from the Internet shall be scanned for viruses prior to being forwarded to the destination and quarantined if infected. In addition, the Contractor shall provide virus protection for all TCE managed equipment to ensure the integrity of the TCE managed network services.

The Contractor shall ensure that the virus signature updates for all TCE equipment are configured to update on a daily basis, and shall also provide update capabilities as follows:

a) A central server located within the Government intranet shall 'push' updates to each TCE-managed and value-added workstation and server.
b) The client on each TCE-managed machine shall be configured to automatically update signatures.

The Contractor shall ensure that the virus protection software will log an event if a virus is detected on the host system. The Contractor shall ensure that the virus protection software shall report to a central alerting station when a virus is detected.

The Contractor shall apply virus patches and software upgrades to device operating systems (OS), as necessary, within the bounds of the TCE environment. The Contractor shall provide the Government with read-level access to all TCE equipment in order to allow Government personnel to audit the software revisions and patch levels to ensure compliance with FedCIRC recommendations. The Contractor shall comply with all FedCIRC recommendations and shall provide proof of compliance in the bi-monthly meeting with the Government.

C.3.1.3.4 Provide Domain Name System Services

The Contractor shall operate and manage physical servers required for providing DNS for 'ustreas.gov' and other similar domain names as required by the Government. The Contractor shall maintain the Government's current DNS structure and shall make recommendations to the Government for any improvement. However, the Government will retain sufficient management control of the DNS infrastructure to update records when required.

C.3.1.3.5 Provide Secure Enterprise E-mail Service

Email is an integral part of Treasury and shall conform to industry standards for interoperability. The Contractor shall provide secure enterprise e-mail services to the Government. The services shall include capabilities for sending, storing, processing, and receiving e-mails and multimedia e-mail attachments. All inbound and outbound e-mails shall be scanned for malicious codes and viruses and shall be cleaned and quarantined, if found infected. Additionally, the e-mail originator shall be notified of any such activity. The Contractor shall maintain the enterprise e-mail service at 99.99% or higher availability.

C.3.1.4 Provide Encryption Service

The Contractor shall provide layer 3 VPN services to secure TCE network traffic passing across or point-to-point on the Contractor's managed network environment. The Contractor's encryption solutions shall possess the ability to support IPSec (in encapsulating security payload mode), Internet Key Exchange, and registered user portal/employee user portal (IRS) functions.

The Contractor's encryption solution shall support the automatic re-establishment of encrypted circuits in the event of an interruption in service.

The Contractor's encryption solution shall not inhibit the use of resilient or redundant hardware, routing, or firewall configurations.

The Contractor's encryption solution shall accept session establishment and authentication based upon industry standard authentication services.

The Contractor's encryption solution shall support Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) algorithms, as specified under the FIPS specifications

C.3.1.5 Secure Physical Assets

The Contractor shall ensure that its equipment and practices comply with all relevant Federal Government policies for protection of physical assets at each site. Refer to C.3.1.2.1, *Comply with Policies and Procedures,* for list of Federal Government policies.

C.3.2 Core Program-Wide Operations and Support Services (OSS) Requirements

C.3.2.1 Conduct Transition From TCS to TCE

A successful transition from the TCS network to the TCE network is absolutely critical to the Treasury and its Bureaus. The Contractor's approach to and execution of this transition will be the most important factor to the Government in evaluating the performance of the Contractor in the base period of this contract. The Government has identified three main features that the Contractor will provide for transition:

a) Risk minimization and mitigation;
b) No compromise of continuity;
c) Strict adherence to the post-award schedule – neither ahead of nor behind schedule will be acceptable to the Government.

The Contractor shall consider seasonal impacts of each Bureau's mission such as, IRS tax season, the last two (2) weeks of September and the first two (2) weeks of October for FMS and BPD, and other similar critical periods for Treasury Bureaus in regard to transition and maintenance. Additionally, the Government expects the transition to be successfully completed by September 27th, 2005.

The Contractor shall agree to meet the SLAs for transition defined under Section F.

C.3.2.1.1 Develop Transition Plan

The Contractor shall prepare and implement a well-defined TCE Transition Plan with the Government's approval. However, the Contractor shall not proceed with transition prior to obtaining Government approval of the Transition Plan in its entirety or in part. The Contractor shall provide an initial Transition Plan with the proposal, which shall include a complete schedule for transitioning all Government sites from TCS to TCE. A final detailed Transition Plan shall be submitted to the Government for approval within 30 days of receiving notice to proceed. The Contractor shall coordinate its proposed sequence for transitioning sites with the Government and shall make adjustments to the sequence, at the Government's direction, prior to making the Transition Plan final. The Contractor shall work with the TCE Program Manager to modify the Transition Plan as needed.

The Transition Plan shall address the Contractor's general approach to and provide a detailed schedule of the proposed transition solution. The Transition Plan shall also define the Contractor's approach to staffing, progress reporting, coordination with third-party vendors, and customer education and communication. The Contractor's Acceptance Test Plan shall be included in the Transition Plan. Additionally, the Contractor shall identify all project management and planning tools that were used to develop the Transition Plan.

The Contractor shall define any pilot or ramp-up activities in the Transition Plan. The plan shall also identify potential risks and the Contractor's mitigation strategies for those risks. Additionally, the plan shall explain how system C&A will be executed in support of transition.

C.3.2.1.2 Conduct Site Surveys

The Contractor shall propose how it will capture site details as a part of the transition, and follow Government site access schedule and access requirements, which will be provided to the Contractor at contract award.

C.3.2.1.3 Transition or Replace Existing TCS Government Equipment

All Government owned TCS equipment will be provided to the TCE Contractor under exchange/sale authority. Any equipment the Contractor uses as part of TCE shall be operated, managed, and maintained at the Contractor's expense, and at no additional cost to the Government. In the event any equipment becomes inoperable, the Contractor shall replace the equipment as necessary to continue to provide seamless managed services under the contract. A list of TCS equipment is supplied in Section J, Attachment J-4. See H.17 *Exchange/Sale*.

C.3.2.1.4 Implement Approved TCE Transition Plan

The Contractor shall implement the approved TCE Transition Plan and shall complete successful transition all Government sites from TCS to TCE by September 27, 2005.

C.3.2.1.5 Conduct Weekly Status Meetings

During the transition period, the Contractor shall coordinate and support weekly status meetings with the Government. During such status meetings the Contractor shall, at a minimum, present to the Government accomplishments, issues, and potential risk areas. The Contractor shall work with the Government's Transition Manager to coordinate facilities and attendance.

C.3.2.1.6 Conduct Pilot Site Transitions

The Contractor shall initially transition a pilot site within each Bureau, as approved by the Government Program Manager (PM). The Contractor shall make a list of all issues encountered during the transition of pilot sites and provide adequate resolution for ensuring seamless transition of sites in future.

C.3.2.1.7 Provide 5 Day Notice of Site Visits

The Contractor shall provide a minimum of five (5) business days advance notice to site point of contact (POC), prior to visiting the site or conducting any changes to the site's service, as part of transition. The Government will grant exceptions where it deems necessary. A list of all site POCs and their profiles will be provided to the Contractor post-award.

C.3.2.1.8 Provide Seamless Transition

During transition to the TCE Network, the Contractor shall be responsible for maintaining continuity of operations with no disruption of service. The Contractor shall coordinate the transition with the PM and affected Bureau such that it does not impact their peak seasonal missions identified in C.3.2.1, and ensure that all platforms are operational with no service interruption during cutover. The Contractor shall notify the site POC before cutover via email, web, phone call, pager, or any other method specified in the POC's profile. In addition, there should be no disruption of communications between sites during transition.

C.3.2.2 Program Management and Reporting

The Contractor shall provide proactive and responsive program management support to the Treasury and the TCE Contract. See Section G for a description of roles and responsibilities within the Treasury's program management structure.

The Contractor shall develop and submit a Program Management Plan (PMP) that addresses, at a minimum, its approach to communication and coordination with the Government, staffing, substitution and retention of key personnel, and change request processes. After contract award, the Contractor shall deliver the final PMP within 60 calendar days of notice to proceed.

C.3.2.2.1 Provide Single Point of Contact

The Contractor shall provide specified points of contact to the Government, as identified in G.3, *Contractor Representatives*, for issue resolution, program management, and other contract issues.

C.3.2.2.2 Quality Control Plan

The Contractor shall develop a comprehensive Quality Control Plan that describes the approach to monitoring and validating the quality of service and adherence to the service levels of all required services and management systems. The plan shall detail the procedures that shall be used to ensure that the Contractor's service and operational and management support systems satisfy all the requirements and service levels of the SOW. The plan shall also include the milestones and measures that shall be used by the Government to determine compliance to the plan.

C.3.2.3 Provide Web-Based Ordering System

The Contractor shall provide and maintain a secure, real-time, web-based ordering system. The system should provide drop-down menus with service options available under TCE and should be linked to the billing system to allow easy tracking of orders. Additionally, the Contractor shall meet the SLAs for order management defined under Section F. Service order procedures are provided in G.4 and G.5.

C.3.2.3.1 Single Ordering System Accessible from All TCE Sites

The Contractor shall provide a single order processing system for all TCE related services. The system shall be web-based and accessible by the PM and Bureau Designated Agency Representative (DAR). A complete list of site IDs will be made available to the Contractor prior to the transition phase. The Contractor shall group and label all service orders using the appropriate site IDs and shall update and maintain an accurate list of site IDs through regular communications with the PM and appropriate Bureau DAR. In the event the ordering system is unavailable due to emergencies, communication failures, etc., the Contractor shall provide the Government with secure fax and voice call based alternatives for placing orders.

C.3.2.3.2 Order Tracking with Prices

The Contractor shall provide the Government with online web-based capability of ordering, tracking, and reviewing all TCE service orders with associated pricing information. The system should allow the PM and Bureau DARs to log into an individual account and check the status of any Bureau-specific order by searching for either the order request or confirmation number. In the event the Contractor discovers any issue(s) with the order, the Contractor shall notify the appropriate Bureau DAR within one (1) business day of discovery.

C.3.2.3.3 Report Orders by Bureau POC

A Bureau DAR is an employee of an agency who has been authorized by his or her respective agency or Bureau to initiate and track service orders. Each Bureau will identify to the Contractor its authorized DAR along with the following information: name, agency represented, current address, telephone number, e-mail address, the services the DAR is authorized to order, and an indication of whether the DAR has expedited ordering authority. The Contractor shall maintain a current directory of all DARs, by Bureau. A Bureau may designate and authorize one or more individuals who are not employees of the Bureau to perform Government POC functions.

The Contractor shall provide Bureau DARs with the capability to view the current status of any or all orders, online and in real-time. The Contractor shall maintain a database of Government DAR profiles that lists the preferred contact method for each DAR when reporting TCE order status and service status messages. Methods of contact shall include either email, pager, or phone call. Moreover, the Contractor shall provide an order status system that lists the status of all orders by the specific ordering profile for that DAR. The Contractor shall provide the Government with the ability to sort and find orders by user ID code, as well as other sort and search criteria associated with the DAR's profile. In addition, the Contractor shall provide the capability of tracking multiple items ordered for a single location through a common order

number. However, this single order number shall also provide the ability to track a subset of items within that order.

C.3.2.3.4 Send Confirmations of New Service Orders

For all newly ordered services, the Contractor shall send confirmations to the DAR via the method specified in the DAR's profile. The method of confirmation shall typically include email, web, phone call, and pager at the DAR's selection. The Contractor shall not send confirmations containing any Sensitive but Unclassified (SBU) information via email, phone call, or web-based tools. Only pre-approved methods for sending SBU information to the Bureau DARs shall be permitted.

In the event the Government needs alternative means of receiving confirmations of orders, the Contractor shall provide the capability to offer custom confirmation methods for exception orders. The custom confirmation methods typically could apply to special projects, special access requirements, and sensitive or high priority orders requiring personal contact with the Bureau DAR. The Government reserves the right to select the method for the Contractor to use for confirmation of these orders.

The Contractor shall respond to the Government within forty-eight (48) hours of submission of a custom order to set a meeting time and date to discus the order.

C.3.2.3.5 Notify POCs of Equipment Arrivals

The Contractor shall send notice to the site POC as identified on the order via email, web, phone call, pager or other type of notification as specified in the POC's profile, of any equipment arrival before one (1) business day of its arrival. The Contractor shall include the shipment date and tracking information on the notification.

C.3.2.3.6 Send Disconnect Notifications

The Contractor shall provide confirmation of a service disconnect request via email to the Government POC for that site. The Contractor shall notify the POC and DAR at least five (5) business days in advance before disconnecting any service to a site. Additionally, the Contractor shall disconnect service and remove any CPE within fifteen (15) business days of receiving a disconnect request. Moreover, the Contractor shall ensure that all physical circuits, services, equipment, etc., associated with a Government-issued service disconnection or cancellation request are completely removed and disconnected. The Contractor shall certify, by sending a message to the site POC via email, web, phone call, pager or any other type of notification as specified in the POC's profile that the service has been successfully disconnected, within 24 hours of completing a service disconnect request. The Contractor shall include a tracking number for the disconnected service in its next invoice. Additionally, the order completion notice must be accepted and verified by the respective site POC and Bureau DAR.

In the event that the Contractor encounters any issue(s) with completing the service disconnect request the Contractor shall notify the site POC of these issue(s) within one (1) business day.

C.3.2.3.7 Service Installation Notification

The Contractor shall send service installation notification to the site POC for each site. The notification shall be web-based, as well as distributed via email and associated with the service order number. In the event of emergencies or same day service, the Contractor shall provide the above information via phone to the site POC prior to the dispatch of the technician(s).

C.3.2.3.8 Order Completion Notification

The Contractor shall provide a web-based order completion notification to the site POC and Bureau DAR within 24 hours of the order completion. The web-based notification shall provide the DAR the capability of either accepting or rejecting the order completion notification via the same web interface. The DAR will either accept or reject the order within two (2) business days of receiving the order completion notification from the Contractor. The notification should include the tracking number of the order that will be reflected in the next invoice.

However, the Government shall have the right to reject any newly installed service(s) at a site in the event the site fails to pass one or more verification tests outlined in the Acceptance Test Plan (ATP), included in the Contractor's Transition Plan, to ensure successful deployment of service(s) at that site. The DAR shall have the ability to notify the Contractor whether he/she has accepted or rejected services at the site through a web interface provided by the Contractor. The Contractor shall not bill the Government for any services that are not accepted by the DAR.

C.3.2.4 Provide Efficient Billing and Invoicing

The Contractor shall provide a secure, real-time, and web-based billing and invoicing function, which will conform to the Government's Prompt Payment Act. Invoice data provided from this site shall be for informational purposes only and shall not constitute an official invoice. Additionally, the Contractor shall agree to meet the SLAs for billing and invoicing defined under Section F. Invoicing procedures are identified in G.9.

C.3.2.4.1 Provide Real-Time Access to Billing Information

The Contractor shall provide functionality that enables the Government to access, review, track, and download bills, billing information, and billing reports in real-time using a web interface.

C.3.2.4.2 Bill on a Monthly Calendar Cycle

The Contractor shall bill separate service charges for each calendar month billing period. In cases where significant cost savings or mutual financial benefits could be realized, the Contractor may propose alternative billing cycle options, such as quarterly or semi-annually, and provide the details associated with such a billing cycle.

C.3.2.4.3 Delay Billing Until Government Accepts Service

Successful installation of circuit(s) and equipment by the Contractor shall not constitute the overall acceptance of service. The Government will conduct both operational and functional tests, according to the acceptance test plan (ATP) included in the transition plan, to ensure that all service components are fully operational before accepting the service at any site. The

Contractor shall not apply billing until the Government the Bureau DAR accepts the service for that site. .

C.3.2.4.4 Provide Billing by Bureau

The Contractor shall bill separate service charges to each Bureau for the services rendered. The Contractor shall provide access to each Bureau DAR to the bills for its own respective services.

C.3.2.4.5 Provide Access to Bill Summaries and Breakouts

The Contractor shall show a summary view of all charges, by Bureau, on its invoice to the Government. The summary view shall show each site ID, the charges, the bandwidth, and the CoS level associated with that invoice. Additionally, the Contractor shall show a detailed view of all charges, by Bureau, on its invoice to the Government. The detailed view shall show all charges and site ID, site category level, class of service, bandwidth, optional security services, and access circuit costs. The Contractor shall provide for standard invoices, with selectable fields from the web-based system for ad hoc reporting.

The Contractor shall clearly highlight on its invoices to the Government any new charges for that month and shall associate such charges with specific service orders. The Contractor shall show on the invoice items such as new features, new services, and service level changes.

C.3.2.4.6 Submit Bills in Multiple Formats

The Contractor shall issue invoices and financial reports using multiple media formats. The multiple media formats shall typically include web-based and downloadable flat files, printed hard copies, and CDs. Additionally, the invoices must be presented in a single billing format, with selectable fields for viewing by individual Bureaus.

C.3.2.4.7 Discontinue Billing Within 30 days

For any service disconnection, the Contractor shall discontinue billing immediately following the disconnection of the service. Credits shall be provided to the Government if billing continues after 30 days of the disconnection date.

C.3.2.4.8 Allow Withholds for Disputed Amounts

The Government reserves the right to withhold a part of or the entire amount being disputed. The Contractor shall allow the Government to enter withhold amounts into the billing system.

C.3.2.5 Provide Management Reporting

The Contractor shall provide the Government real-time web-based visibility into network management statistics and network configuration information for the TCE Network. The visibility shall include, but is not limited to, view of network performance statistics, capacity utilization, fault management, health monitoring, and similar information. Additionally, the Contractor shall provide reports on the above both on a regular and ad hoc basis. The Government shall have the right to audit any of the above information provided by the Contractor at any time. The

Contractor shall provide the Government with all necessary access to the facility, equipment, reports, and other information required to carry out the audit.

C.3.2.5.1 Managed Network Services Reports

The Contractor shall provide detailed network management reports, showing Week-To-Date, Month-To-Date, and Year-To-Date statistics. The Contractor shall make the reports available on the TCE web site and shall, at a minimum, include the following:

A) Access circuit and router statistics (for each site):
1. Peak bandwidth utilization
2. Hourly average bandwidth utilization
3. Edge/access router CPU utilization
4. Average ping response time between the site access router and the nearest core backbone router
5. Average ping response time between two pre-defined access routers (within each Bureau)
6. Traffic breakdown up to the port level e.g., HTTP, FTP, etc., (along with the bandwidth consumed and the source and destination IP addresses)

B) Backbone circuit and router statistics:
1. Peak bandwidth utilization of all Government's traffic between core backbone routers
2. Hourly average bandwidth utilization
3. Average ping response time between core backbone routers

The mechanism for measuring utilization is provided in Section F. The Contractor shall meet with the Government bimonthly to provide and discuss utilization and trending reports, and capacity planning services to maintain and improve service levels for each site. The Contractor shall provide automated alerts to the Government when average utilization exceeds 60% of total capacity at any site. The Contractor shall include this site in the bimonthly utilization and trending reports and recommend actions for improving its capacity and performance. Additionally, the Contractor shall notify the Government of any access circuit utilization exceeding 30% for four (4) or more hours per day at any site for five (5) or more days in a month.

C.3.2.5.2 Security Services Logs and Reports

The Contractor shall ensure that the firewalls and intrusion detection systems (IDS) provide audit log tracking of all client transactions (including all NIST 800 series recommended data elements) and provide audit log access to the appropriate Government personnel. The Contractor shall ensure that the log files are provided to the SOC through a secure data feed. The archived audit logs shall be maintained for a minimum of five (5) years, and are subject to recall by appropriate Government personnel.

The Contractor shall ensure that the firewall and IDS are capable of displaying event information and sending management and event statistics to a centralized management tool/server. Additionally, the central management tool/server shall be able to generate customized reports of event information in both raw (e.g., comma delineated, etc.) and web-based formats and shall be compatible with security management system applications.

C.3.2.5.3 Send Automated Alarm Notifications

The Contractor shall automate sending alarm notifications to the Government for any network performance degradation and security breaches. The Contractor shall ensure that this notification takes place using both voice and e-mail. The thresholds for email notification shall be coordinated with the Government. In addition, the Contractor shall generate advisory email messages to the affected Bureaus when network service affecting issues are detected.

The Contractor shall provide the capability to the PM and Bureau DARs for updating the alarm notification database. As missions change, the Government shall coordinate with the Contractor to identify new threshold levels.

C.3.2.5.4 Provide Configuration Management Reporting

The Contractor shall provide real-time read-only views into configuration settings for all provider equipment (routers, switches, firewalls, IDS, etc.) for the TCE network. The Contractor shall provide an on-line web-based method for submitting network configuration requests.

C.3.2.5.5 Archive System Events

The Contractor shall store all system event log files for firewalls, IDS, smart switches, and routers for one (1) year using on-line media, and for at least two (2) additional years on off-line storage media and as per guidelines mentioned in TD80-01 and TD80-05. Firewall audit logs shall be stored for Government review for a period of five (5) years.

C.3.2.5.6 Conduct Periodic Status Meetings

After the transition period, the Contractor shall conduct bimonthly status meetings during the first year of the contract and quarterly meetings thereafter.

C.3.2.6 Provide Help Desk Support

The Contractor shall provide help desk support for receiving, reporting, and resolving trouble calls related to services provided under the TCE Contract. The Contractor shall provide world-class user technical assistance via desk-side service, phone, e-mail, or fax for solving information technology service-related issues to the user's complete satisfaction. This shall include providing an integrated service with a single point of contact for all Treasury users. Designated Treasury shall have the capability to interact or communicate with the Help Desk by voice, e-mail, fax, web, and shall have visibility into a web-based trouble ticket status system. The Government anticipates required help desk support to be minimal, once a site is fully operational. The help desk support provided by the Contractor for each site category shall be as follows:

1) Category-1 Sites: The Contractor shall provide 24 hours a day and 7 days a week (24 x 7) help desk support to all Category-1 sites. The hours of support shall be round the clock on business days, weekends and holidays 365 days during regular years or 366 days during leap years.
2) Category-2 Sites: The Contractor shall provide 12 hours a day and 7 days a week (12 x 7) help desk support to all Category-2 sites. The hours of support shall be

between 7 am to 7 pm local time on business days, weekends and holidays 365 days during regular years or 366 days during leap years.

3) Category-3 Sites: The Contractor shall provide 9 hours a day and 5 days a week (9 x 5) help desk support to all Category-3 sites. The hours of support shall be between 8 a.m. to 5 p.m. local time Monday to Friday each week year round.

The Contractor shall provide the above three categories of help-desk support services using a single help-desk infrastructure. The Contractor shall provide help desk technical support at the same quality during holidays, weekends, and regular business days. Additionally, the Contractor shall agree to meet the SLAs for help desk support as defined under Section F.

C.3.2.6.1 Trouble Ticket Reporting and Escalation Plan

The Contractor shall provide a centralized telephone number for reporting trouble calls pertaining to services provided under the TCE Contract. The Contractor shall identify and define trouble ticket terminology with the Government.

The Contractor shall develop and submit an Escalation Plan that describes trouble ticket priority levels and the escalation process. The Contractor shall provide escalation service with procedures to be reviewed and approved by Treasury and implemented by the Contractor. These services shall include the timely notification of Treasury personnel by help desk staff of planned or unplanned system maintenance or degradation of TCE services. Upon notification of TCE service outages, either through electronic or user notification methods, the Contractor shall escalate unresolved issues in accordance with escalation procedures as defined in the Contractor's escalation plan. The Escalation Plan shall also address immediate Tier 3 or equivalent support for resolving major outages.

The trouble ticket priority system shall be synchronized with the National Communications System (now part of Department of Homeland Security), Telecommunications Service Priority levels, and the Emergency Preparedness/COOP facilities within Government and the Bureaus' COOP and DR Plans.

C.3.2.6.2 Notification of Potential Problems

The Contractor shall be proactive in handling recurring troubles, security incidents and issues, unresolved trouble calls, delayed service delivery, billing issues, and other issues that result from the TCE Contract. The Contractor shall notify the PM and Bureau DARs, by email or phone call, of any problems occurring within the Contractor's network that could potentially affect quality of service or availability of the TCE sites.

C.3.2.6.3 Official Inquiries Response Within 24 Hours

If the Government submits a written inquiry regarding an unresolved issue(s), the Contractor shall respond in writing within 24 hours. The Contractor shall identify the source of the problem, it's current status, and a projected timeframe for its resolution.

The Contractor shall propose additional mechanisms for trouble ticket resolution that considers timeliness, customer service, and remedy for unresolved and/or recurring issues.

C.3.2.6.4 Pre-Approve Maintenance in Accordance With Guidelines

The Contractor shall provide maintenance for all TCE equipment according to the guidelines outlined in Table C-1:

Table C-1: Maintenance Guidelines

Description	Guidelines
Routine maintenance window	The Contractor shall propose a standard maintenance window for performing normal maintenance activities. This maintenance window shall be either between 10pm-4am (Sun-Thu.), or between 10pm-6am (Fri-Sat), including federal holidays.
Quarterly maintenance review	The Contractor must submit a quarterly maintenance review schedule for coordination with the TCE Program Management Office and Bureaus. The Contractor shall provide quarterly maintenance schedules for routine maintenance activities 15 days before the start of each quarter.
Unscheduled maintenance notification	The Contractor shall notify the Government before performing any emergency maintenance activities on the network.
Busy season avoidance	The Contractor shall delay doing maintenance and updates on TCE network during emergencies declared by TCE, and at the Government's request. The Contractor shall not conduct maintenance during busy seasonal periods (e.g., tax season).
Maintenance activity approval	The Contractor shall not perform any TCE maintenance activities that impact service, unless the Government has approved the activities.
Suspension of scheduled maintenance activity	The Contractor shall suspend scheduled maintenance activities at the Government's request to accommodate special situations.

The Contractor shall develop and submit a maintenance plan that outlines maintenance schedules and notifications between the Contractor and the Government. The plan shall include, at a minimum, requirements specified in Table C-1, Maintenance Guidelines.

C.3.2.7Host TCE Web Site

The Contractor shall establish and maintain a TCE web site within the Government intranet architecture. The TCE web site shall, at a minimum, enable program information sharing and viewing of operations status, trouble ticket status, invoice records, and service ordering status. If the Government requires customization of the web site, then the Contractor shall follow Government intranet policy for design, operation, navigation, search, content architecture, and content management practices. The web site shall:

a) Adopt Government access control practices,

b) Use the Government Public Key Infrastructure (PKI) for digital signature and authentication for order placement, information access, and work approvals

C.3.2.8 Provide Enterprise-wide Directory Services

The Contractor shall provide, deliver, and maintain global information services throughout the Treasury operating environment. These services should support the management and

utilization of file services, network resources, security services, electronic messaging, web, e-business, white pages, and object-based services across the Treasury.

Information services shall include storing, updating, and publishing directory information from multiple systems and formats including e-mail addresses, commercial and DTS telephone numbers, certificates, addresses, applications, network devices, documentation and routing information, as well as other data and/or resources in support of the entire Treasury IT environment. The Contractor shall ensure directory entries conform to Government standards and provide the flexibility to include users not directly supported by the Contractor. This enterprise-wide directory services shall support the ability for end users to interact globally at anywhere and anytime with the network directory services in a transparent and consistent manner. The directory services offered shall support and facilitate the following basic functions:

a) Supported by PKI authentication services, provide the capability for users, devices and applications to discover and utilize information services data for electronic authentication and identity management
b) Support the monitoring of administration and management of network resources
c) Support the implementation of global account management and subsequent authentication and authorization to data maintained in the global directory service
d) Support the enablement and distribution of applications
e) Provide a proactive environment that builds and manages relationships between objects within the global directory service

C.3.2.8.1 Maintain and Operate Treasury Directory System (TEDS)

The Contractor shall assess whether the Treasury should migrate to the TCE Contractor-provided enterprise-wide Directory Services or continue with its existing Siemens-based directory service. If the Contractor deems it necessary to continue with the Siemens-based directory system, then the Contractor shall maintain and operate the existing Siemens-based directory system and current directory architecture. Detailed information about the Treasury Directory System (TEDS) is provided in Section J.

The Contractor shall operate and maintain a X.500-based (and LDAP) TEDS as an infrastructure utility while providing at least 99.99% availability. The Contractor shall transition operation and maintenance of the TEDS system from the TCS incumbent Contractor to its TCE environment without disrupting any services if the Siemen-based product is continued.

The Contractor shall maintain a TEDS back-up architecture, which includes back up sites for TEDS, shadows, and connectivity between masters, back up, and the shadows. The support should also include the following:

a) Administer commercial-off-the-shelf (COTS) product licenses and renewals
b) Operate and maintain the utility
c) Assist customers in directory content updates
d) Offer customer support for fault management and service restoration
e) Enable application access
f) Develop enhanced applications for accessing TEDS
g) Interface with Government PKI Certificate Authority
h) Support Bureau content refresh or structural changes

In addition, the Contractor shall provide help desk support for the TEDS utility via the Enterprise-wide network and security operations center. This support should ensure technology refresh of the various TEDS COTS hardware and software products on a cyclical basis. In addition, the Contractor shall ensure that the COTS products are maintained at latest patch, release, and version levels.

C.3.2.9 Provide Data Feed to Security Operations Center

The Contractor shall provide the following data feeds from the TCE NOC to the Government's Security Operations Center (SOC):

a) A feed of ID sensor outputs
b) A feed of firewall audit logs and alarms

The Contractor shall be responsible for establishment and operation of the links supporting these data feeds from TCE NOC to the Government SOC. Additionally; the Contractor shall ensure that the data provided through these feeds is compatible with Government's reporting capabilities at the SOC.

C.3.3 Core Site-By-Site Technical Requirements

C.3.3.1 Provide End-to-End Managed Network Services

The Contractor shall provide fully managed end-to-end bandwidth services to all TCE sites listed in Attachment J-2. The bandwidth shall be provided in the following increments, as ordered by the Bureau DAR:

a) 128 Kbps
b) 256 Kbps
c) 512 Kbps
d) 1 Mbps
e) 1.544 Mbps
f) 3 Mbps
g) 6 Mbps
h) 9 Mbps
i) 10 Mbps
j) 12 Mbps
k) 15 Mbps
l) 20 Mbps
m) 30 Mbps
n) 45 Mbps
o) 100 Mbps
p) 155 Mbps
q) 622 Mbps
r) 1 Gbps
s) 2.4 Gbps
t) 10 Gbps

The Contractor shall meet the site-specific SLAs defined under Section F.

C.3.3.1.1 Interface to Local Government Equipment, as Required

The Contractor shall operate and manage all hardware and software components up to the demarcation point depicted in Figure C-2.

The Contractor shall provide one or more 10/100 Mbps or 1/10 Gbps Ethernet interface(s) to interface with the Government interface equipment in accordance with local requirements at each site. Prior to the actual installation the Contractor shall determine requirements for space and power for supporting the CPE at each TCE site. However, the Contractor shall comply with Government's physical plant requirements, such as physical space, rack space, power, and HVAC for installing the CPE at the TCE sites. In addition, the Contractor shall provide all equipment and accessories required to install and maintain the CPE at all TCE sites. This shall include, but is not limited to racks, cables, tools, etc.

The Contractor shall label and run cable according to Government guidelines in locations where a cable extension is required to connect a TCE circuit to the Government-specified demarcation point. The Contractor shall follow Government guidelines and local procedures to access, install and maintain all TCE equipment at all locations.

C.3.3.1.2 Provide Public IP Addresses and Support Legacy Protocols

The Contractor shall provide public IP addresses as required to support TCE managed network services. The Contractor shall not require the Government to renumber their current IP addressing scheme to take advantage of any present or future service offerings.

The Contractor shall provide support for all legacy protocols required by the Government. This shall include support for the following protocols at a minimum:

Table C-2: Legacy Protocols

Network Protocols	Routing Protocols
IP	OSPF
Novell IPX	RIP
SNA	Other legacy protocols
X.25	BGP

C.3.3.1.3 Provide Class Of Services and Meet End-To-End SLAs

The Government has designated all TCE sites as belonging to one of the three categories with each category of site requiring a different availability as follows:

a) Category-1 Sites require ≥ 99.99% availability
b) Category-2 Sites require ≥ 99.9% availability
c) Category-3 Sites require ≥ 99.0% availability

The Government has identified three CoS types for various traffic types. Table C-3, summarizes the demarc-to-demarc SLA parameters, [latency or round-trip time (RTT), jitter, and packet loss], associated with each CoS. Section F provides the definition, performance measures, and measurement mechanisms for the CoS SLA parameters. Each site will have a mix of Class of Services, which shall be provided either over the same physical circuit or over multiple circuits, as per architecture of the site. The Contractor shall agree to provide managed services in accordance with the demarc-to-demarc CoS SLA parameters outlined in Table C-3 and described in detail in Section F. The CPE is not required to support any additional features

for supporting the applications type. However, the future TCE network architecture must support secure ubiquitous access to all enterprise IT resources utilizing advanced protocols (IPv6, etc.) that support the convergence of data, voice, video and multimedia services over a highly available robust network transport infrastructure.

Table C-3: Class of Services

Class of Service	Application Type	Latency (RTT)	Jitter	Packet Loss
CoS-1	Voice over IP, video conferencing, etc	≤ 125 ms	≤ 25 ms	≤ 0.1 %
CoS-2	Non-real-time traffic requiring better than standard service, video streaming, SNA, and other Government enterprise-wide applications such as HR Connect, etc	≤ 175 ms	≤ 35 ms	≤ 1.0 %
CoS-3	Regular business traffic like email, http, ftp, etc.	≤ 250 ms	≤ 45 ms	≤ 2.0 %

The Contractor shall provide the capability to adjust the CoS, and to provide pricing based on the CoS for each TCE site, as shown in the pricing CLINs in Section B.

C.4 ENHANCED SERVICES

C.4.1 Program Wide Enhancements

This section describes additional services that the Government may require. The Contractor shall include adequate information in the proposal to demonstrate its capabilities to provide and support these services. The procedures for ordering enhanced services are described in G.5, *Special Projects*.

C.4.1.1 Special Projects Support

The Contractor shall support special projects outside of managed WAN services on a Fixed Price or Time and Materials (T&M) basis as requested by the Government. The Contractor shall respond to requests from the Government to submit these projects in accordance with the procedures provided in G.5 of this contract.

C.4.1.2 Link Encryption

The Contractor shall provide support for existing link-encrypted circuits currently used by the Government to interconnect IRS data centers. Link-encryption is required for certain

Government's legacy SNA applications and shall be provided on private point-to-point links between the IRS sites specified in Section J, Attachment J-2. The Contractor shall ensure that the link encryption solution shall be compatible with existing legacy IRS applications and shall be supported until IRS upgrades these applications to operate under/using standard TCE core services.

The Contractor's encryption solution shall comply with all relevant federal regulations, including FIPS 140-2 governing the use of cryptographic-based security systems to protect sensitive information in computer and telecommunication systems.

C.4.1.3 Provide Web Hosting Services

In the event the Government requires web hosting services under this contract, the Government will request that the Contractor submit a proposal to provide these services in accordance with G.5.

If tasked to provide web hosting services, the Contractor shall provide the facility, physical security, HVAC, fire protection, uninterruptible power, service isolation, facility alarms, host equipment, and software up to and including the hardware operating system. In addition, the Contractor shall provide COTS application products residing above the server operating system at the Government's election.

C.4.1.4 Host and Operate Public Key Infrastructure (PKI)

In the event the Government requires PKI hosting services under this contract, then the Government will request that the Contractor submit a proposal to provide these services in accordance with G.5.

C.4.1.4.1 Host Treasury's Public Key Certificate Authorities

In the event the Contractor is tasked to provide PKI services, the Contractor shall host the Treasury's Public Key Certificate Authorities (PKCA) such as root, operational, and external. The Contractor's solution shall provide continuity in the existing Entrust PKI architecture.

If tasked to provide PKI services, the Contractor shall serve as the Government's agent for the administrating Certificate Authorities (CA) to ensure ongoing trust of the CAs and cross-certification with the Federal Bridge.

C.4.1.4.2 Provide System Administration Support

In the event the Government requires system administration support, the Contractor shall provide such support using cleared personnel to ensure system backup, test back-up recovery, process certificate revocations, install patches, and perform upgrades to release software to the environment.

If tasked to provide system administration support, the Contractor shall serve as the Government's Designated Agency Representative (DAR) for administration of the PKCA hosting services provided. As the DAR, the Contractor shall monitor the hosting service, independently verify and validate invoices for the hosting service, place orders for service changes, and administer service delivery.

C.4.1.4.3 Transition of Existing PKI Infrastructure

As requested by the Government, the Contractor shall transition the hosting and administration of the PKI Certificates from the current hosting service to the Contractor's hosting service. This shall be accomplished in accordance with Contractor-developed and Government-approved transition, concept of operations, and personnel and industrial security guidelines. The Contractor shall be required to provide a solution for a warm back up PKI hosting of the PKCA. The Contractor's plan shall include content synchronization and a DR Plan.

C.4.1.4.4 Single Sign-On Capability

As requested by the Government, the Contractor shall provide a single sign-on feature in the context of the Government authentication and identity management solution being adopted outside of TCE.

C.4.1.5 Provide Secure Remote Access

In the event the Government requires remote access, the Contractor shall provide a secure remote access solution, which could be integrated into the TCE network in the future. The solution shall include encrypted, authenticated, and non-repudiated VPN based remote access over the Internet to the TCE for authorized Government users via broadband, wireless, dial up, or any other approved access method, and shall use encryption technology that is FIPS certified.

If tasked to provide remote access, the Contractor shall ensure that the remote access method will support centralized authentication and user management. The Contractor shall also ensure that the authentication methods used comply with existing federal and Treasury guidelines.

The Contractor shall ensure that the VPN application and/or hardware is compatible with existing Government core operating systems and applications and must also meet security requirements listed in C.3.1.2.1.

C.4.1.6 Optional Back Up Storage Service

In the event the Government requires back-up storage, the Contractor shall provide a range of back up, restoration and archiving, and off-site storage services that are industry standard or that are, for example, commercially available technologies. The storage services shall ensure survivability and recovery of hosted data, program, and other content and infrastructure.

C.4.1.7 Other Future Services

The TCE network infrastructure shall support, in the future, integration of multiple media, which shall enable users to retrieve and send voice, fax, and email from a single user interface. The Government may elect to deploy the following services in the future:

a) Unified Messaging
b) Secure Enterprise Instant Messaging

The Contractor shall ensure that the TCE network infrastructure is equipped to support the above services at the time of their deployment.

C.4.2 Site-by-Site Service Enhancements

The Contractor shall offer the following services on an a la carte basis. The Government management at each site may choose to exercise all or part of the work contained in this section.

C.4.2.1 Firewall Protection

Individual sites may elect to have firewall services established at the managerial boundary of their organization. Government Bureaus may require the Contractor to implement additional firewall services at the site or Bureau level that meets the following service level standards:

1) The Contractor shall ensure that only authenticated inbound traffic on explicitly approved ports will be allowed to establish connections to Government workstations and servers.

2) The Contractor shall monitor all inbound and outbound connections and traffic at the firewall boundaries and generate audit logs, which shall capture at a minimum source and destination IP address, date and time, and other relevant system information. These audit logs shall be available for Government review for a period of five (5) years. The Contractor shall provide all audit logs to the Government upon Contract completion.

3) The Contractor shall provide firewall solutions that provide stateful inspection and application of proxy-based services. Other firewall inspection methods may be used in addition to ensure network integrity.

4) The Contractor shall ensure that the firewalls have the capability to filter based on all of the following:

    a) Transmission Control Protocol
    b) User Datagram Protocol
    c) IP Addresses
    d) Incoming Network Interfaces

5) The Contractor shall ensure that the firewall shall block all inbound traffic unless that traffic is explicitly permitted.

6) The Contractor shall ensure that the firewall solution shall support a centralized policy management solution.

7) The Contractor shall filter inbound traffic to the TCE Network to reject the following:

    i) Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself

j) Inbound traffic with a source address indicating that the packet originated on a network behind the firewall
k) Inbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks
l) Inbound traffic from a non-authenticated source system containing SNMP traffic
m) Inbound traffic containing IP source routing information
n) Inbound or outbound network traffic containing a source or destination address of the local host
o) Inbound network traffic containing a source address of 0.0.0.0 or outbound containing a destination address of 0.0.0.0
p) Inbound or outbound traffic containing directed broadcast addresses

The Contractor shall ensure that the firewall shall support centralized user authentication and centralized security event logging.

C.4.2.2 Intrusion Detection Services

When directed by the Government, the Contractor shall monitor inbound and outbound traffic at selected TCE sites using IDS technologies that provide for the detection of signature, anomaly, behavior events or use any other federally approved detection method within the client site.

C.4.2.3 Virus Protection

When directed by the Government, the Contractor shall provide additional virus protection services at selected TCE sites. The virus protection service shall be provided within the CPE demarc only.

The Contractor shall apply virus patches and software upgrades to device operating systems (OS) and ensure that virus signature files are kept current on TCE equipment, as necessary, within the bounds of the TCE environment. The Contractor shall not be responsible for site and desktop equipment downstream of the CPE demarc. The Contractor shall ensure that all inbound email traffic is scanned for viruses prior to being stored in the user's mailbox and quarantined if infected. The Contractor shall provide the Government with read-level access to all CPE devices in order to allow Government personnel to audit the software revisions and patch levels to ensure compliance with FedCIRC recommendations.

C.5 SECTION 508 COMPLIANCE

The Contractor shall ensure that electronic and information technology (EIT) services provided under TCE fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR Part 1194. The Contractor shall make available full details of compliance at the Government’s request.

The Contractor must ensure that all EIT services and products that are less than fully compliant are offered pursuant to extensive market research, which ensures that they are the most compliant products and services available to satisfy this contract's requirements.

For every EIT product accepted under this contract by the Government that does not comply with 36 CFR Part 1194, the Contractor shall, at the discretion of the Government, make every effort to replace or upgrade it with a compliant equivalent product or service, if commercially available and cost neutral on either the planned refresh cycle of the product or service, or on the contract renewal date, whichever shall occur first.

Information about Section 508 can be obtained at **www.section508.gov**.

C.6 DELIVERABLES

The Contractor shall provide all deliverables as described herein in accordance with Table C-4 below.

Table C-4: Summary of Deliverable Plans

Plan	Paragraph Reference	Due Date	Update Frequency
Security Tests and Evaluations (ST&E) Plan	C.3.1.2.3	Within 60 days after notice to proceed	Not applicable
Continuity of Operations (COOP) Plan	C.3.1.2.4	Within 60 days after notice to proceed	Semi-annually
Disaster Recovery (DR) Plan	C.3.1.2.4	Within 60 days after notice to proceed	Semi-annually
Program Management (PMP) Plan	C.3.2.2	With proposal submission	Within 60 days of notice to proceed
Transition Plan	C.3.2.1.1	With proposal submission	Within 30 days of notice to proceed
Maintenance Plan	C.3.2.6.4	With proposal submission	Within 10 business days of any change
Acceptance Test Plan	C.3.2.1.1	With Final Transition Plan	Semi-annually
Escalation Plan	C.3.2.6.1	With proposal submission	Within 10 business days of any change
Quality Control Plan	C.3.2.2.2	With proposal submission	Within 10 business days of any change